Analysis of the PPTP and IPSec protocols in Virtual Private Networks

(HS-IDA-EA-00-110)

Thorir Tryggvason (a96thotr@student.his.se)
Institutionen för datavetenskap
Högskolan i Skövde, Box 408
S-54128 Skövde, SWEDEN

Examensarbete på programmet för systemprogrammering under vårterminen 2000.
Handledare: Mikael Berndtsson
Analysis of the PPTP and IPSec protocols in Virtual Private Networks
Submitted by Thorir Tryggvason to Högskolan Skövde as a dissertation for the degree
of B.Sc., in the Department of Computer Science.

June 13th 2000
I certify that all material in this dissertation, which is not my own work has been
identified and that no material is included for which a degree has previously been
conferred on me.

Signed: ______________________________________________________
Analysis of the PPTP and IPSec protocols in Virtual Private Networks
Thorir Tryggvason (a96thotr@student.his.se)

Keywords: Data communications, VPN, PPTP, IPSec, networks, telecommuters, security.

Abstract

Today increasing numbers of individuals are working away from the ordinary workplace while still requiring access to the server located at the workplace. New technology is meeting this demand allowing for safe and secure transmission of the data over the Internet. The aim of this project is to analyse two protocols that are used within the Virtual Private Network (VPN) structure today, with the focus on installation, transmission speed on both Local Area Networks (LAN) and via telephone line and security aspects of the protocols.

The results show that it is quite complicated to setup a VPN network and to get operational. The results also show that there are security compromises within the VPN structure that indicate that if proper precaution is not taken it may give a false sense of security, where the user believes that it is a secure communication when in reality it is not.
Contents

1 Introduction ........................................................................................................ 1

2 Background .......................................................................................................... 3
  2.1 Protocol suites ................................................................................................. 3
    2.1.1 VPN with IPSec ....................................................................................... 3
    2.1.2 VPN with PPTP ....................................................................................... 9

3 Problem description ............................................................................................. 15
  3.1 Yesterday’s Internet ....................................................................................... 15
  3.2 Tomorrow’s Internet ..................................................................................... 17
  3.3 IPSec and PPTP VPNs .................................................................................. 19

4 Methods .............................................................................................................. 21
  4.1 Evaluating installation and encryption ......................................................... 21
  4.2 Evaluating security ....................................................................................... 23

5 Analysis ............................................................................................................... 24
  5.1 The installation phase ................................................................................... 24
    5.1.1 The PPTP trial ....................................................................................... 24
    5.1.2 The IPSec trial ..................................................................................... 28
  5.2 Transmission speeds ..................................................................................... 32
  5.3 Security of the two protocols ........................................................................ 35
    5.3.1 The PPTP security aspects ..................................................................... 35
    5.3.2 The IPSec security aspects ..................................................................... 36
    5.3.3 Security comparison .............................................................................. 37

6 Conclusion .......................................................................................................... 39
  6.1 Suggestions for future work .......................................................................... 40
    6.1.1 NetXray ................................................................................................. 41
    6.1.2 Simulation settings .................................................................................. 42

Acknowledgement ................................................................................................. 44

References ............................................................................................................. 45

Glossary ................................................................................................................ 46
1 Introduction

In today’s international and computer intensive environments, more and more information needs to be sent between two parts and the Internet is the natural bearer of information. Internet is used by millions of people and companies to transmit and receive information. Many companies are relying on a fast, safe and accurate delivery of data through the Internet for their survival.

The Internet is open to just about anyone. This means that all information that is sent from one place to another with the aid of the Internet can be eavesdropped. The consequence is that sensitive information cannot and should not be sent through the Internet without being protected in some way. Today, there are several different methods available to protect and secure information, depending on what the goal is, i.e. what is to be secured. According to Kosiur (1998) a Secure Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) are used to secure e-mail and Secure Sockets Layer (SSL) and Secure HTTP (SHTTP) are used for web applications. With use of keys and authentication systems it is possible to acquire some protection and security in a system that sends messages between two computers on the Internet. By using leased lines and the Internet as a bearer of information that is sent with different applications such as e-mails, using programs like Pretty Good Privacy (PGP) to encrypt the messages. Using leased lines to send information between end points to create an end-to-end tunnel is an alternative way to send information instead of using the Internet. Using the Internet as a bearer with an encrypted message transmission namely Virtual Private Networks (VPN) is an excellent way to securely convey information from point-to-point.

Encryption of some kind of the application information before it is sent is not uncommon; this is to protect the integrity of the message being sent. Recently a new technology has been emerging that is called VPN or Virtual Private Networks (Kosiur, 1998). The information that is to be sent will then be sent in a secure tunnel on the Internet that is created by the VPN. The tunnel allows the information to be transmitted safely and securely through the Internet or any other medium.

The increased demand for secure access to a corporate mainframe or servers in one location has introduced the VPN networks. VPN doesn’t really replace any previous protocols but is rather a new way of sending encrypted information as opposed to using leased lines. The need to connect branch offices to main offices, sometimes in another part of the country and exchange a large amount of data is the ideal situation for a VPN network. VPN offers a cost effective and secure connection between two points, as an alternative to leased lines where a corporation would resort to leasing lines which is more expensive if there are long distance calls to be made. Corporations that employ telecommuters and mobile employees can use VPN to let them safely access the corporate servers without compromising security or data integrity on accessing the information that is kept on the corporate server.

VPN can be applied to vital information flow such as business agreements, governmental information and patient information. Such information as previously named can be used against individuals, governments and corporations in a malicious manner. It can therefore be vital that such information can be encrypted and safely...
sent between two computers. VPN offers a solution to this problem by using the Internet as a transport medium.

The aim of this work is to analyse two of the four protocols that are used with VPN, i.e. Point-to-Point Tunnelling Protocol (PPTP) and IP Security protocol (IPSec). There are several things that will be evaluated during the analysis of the protocols. The ease of installation of the protocols and how complicated it is to get the protocols up and running. That is to install the protocols and see to that they function properly. Another aim is to see if the PPTP and IPSec protocols can acquire the same encryption speed with software based encryption over different bandwidths and with different file types. If they differ in speed, which algorithm is the one that provides better and faster encryption? The third aim is to evaluate how the protocols differ on security aspects, such as key sizes, ease of cracking and encryption strength.
2 Background

The main hardware components of a VPN consist of the computers that interact, a transmission medium, and software or hardware components to encrypt the information with different architectures and methods. Several protocol suites are used with a VPN. The most common are IP-Security (IPSec), Point-to-Point-Tunnelling-Protocol (PPTP) and Layer-2-Tunnelling-Protocol (L2TP) (Kosiur, 1998).

Today there are few alternatives to Virtual Private Networking. One is to lease dedicated lines that will carry the information from point A to point B. The cost that is inevitable when leasing a line maybe from one country to another and the fact that the bandwidth of a leased line is often very small reduces the benefits of the investment. This often results in extremely high telephone bills. The other alternative is to send the information without any encryption; this is often not a feasible alternative since the information may be confidential. The material that is included in chapter 2 is mainly based on information from Kosiur (1998), Stallings (1999), Brown (1999) and various white papers.

2.1 Protocol suites

There are several protocols available to encrypt a message. Some encrypt at the network layer like IPSec while other such as PGP and SSL encrypt at the application layer on the Open System Interface (OSI) model seen in Figure 1. PGP and SSL offer the user to select sites that are allowed and disallowing links to untrusted sites, encrypting the packages that leave the site and authenticating the ones that come in to the site. The benefits of using IPSec over high-level architectures are that secure networking is accomplished not only for selective applications but also for security-ignorant applications. The further down the OSI stack the VPN technology is implemented the better, since it gives better protection against a wider area of attacks. At the same time it can create problems on program interaction at the application level, it is possible to avoid this problem by writing carefully the communication link through the layers in the program.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Application layer</th>
<th>Applications, Netscape, Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 6</td>
<td>Presentation layer</td>
<td>Describes the syntax of data being transferred, FTP, HTML</td>
</tr>
<tr>
<td>Layer 5</td>
<td>Session layer</td>
<td>Request and retry on packet handling</td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport layer</td>
<td>Quality and retransmission issues</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network layer</td>
<td>Addressing and routing issues</td>
</tr>
<tr>
<td>Layer 2</td>
<td>Data link layer</td>
<td>Framing and addressing of packets</td>
</tr>
<tr>
<td>Layer 1</td>
<td>Physical layer</td>
<td>Decides cables and connections</td>
</tr>
</tbody>
</table>

Figure 1. The OSI model. Adapted from Halsall (1995:15).

2.1.1 VPN with IPSec

IPSec uses two different headers in IP packets, which are the fundamental unit of communication in IP networks. The IP packet includes information on the source and the destination as well as the type of data being carried. IPSec defines two types of headers for IP packets to handle authentication and encryption. The Authentication
Header (AH) is designed for authentication purposes, while Encapsulating Security Payload (ESP), is designed for encryption purposes. Only an explanation of the use of AH and ESP with the Internet Protocol version 4 (IPv4) and not the IPv6 protocol will be made. This is because that the IPv4 protocol is currently more used than the IPv6 protocol.

IPSec is built on a number of standardised cryptographic technologies that provide confidentiality, data integrity, and authentication. This can be summarised in the following list (Kosiur, 1998):

- Diffie-Hellman key exchanges to deliver secret keys between peers on a public net. Diffie-Hellman key exchange is the first published public-key algorithm. It appeared in a paper by Diffie and Hellman that defined public-key cryptography (Stallings, 1999).
- Public-Key Cryptography for signing Diffie-Hellman exchanges to guarantee the identities of the two parties and avoid man-in-the-middle attacks
- Data Encryption Standard (DES) and other bulk-encryption algorithms for encrypting the data.
- Keyed hash algorithms (Hashed Message Authentication Code (HMAC), Message Digest, version 5 (MD5), and Secure Hash Algorithm (SHA)) for authenticating packets.
- Digital certificates for validating public keys.

IPSec encompasses three functional areas: authentication, encryption and key management (Stallings, 1999). The authentication mechanism guarantees that the received packet originates from the source listed in the packet header. It also ensures that the packet has not been tampered with during transit. The confidentiality part enables communicating Data Terminating Equipment (DTE) to encrypt messages to prevent unauthorised access to the messages. The key management deals with the secure exchange of keys between the DTEs. All of these agreements have been bundled into a Security Association (SA). A SA includes all necessary information to be able to communicate securely with someone else, including key change information, what algorithms are to be used and how often keys should be changed during one session.

The AH was designed to provide the significant authentication services needed by the IPSec protocol. The AH contains a cryptographic checksum for the packet header. It’s inserted into the packet between the IP header and the rest of the contents of the packet. No changes are made to the content of the packet, where the Transmission Control Protocol (TCP) and IP header remain a fixed size and only the data field is changed to a smaller size to fit in the AH. This is illustrated in Figure 2. The AH contains five fields: the Next Header field which is in all IP headers, a payload length (data), the Security Parameter Index (SPI), a sequence number, and authentication data. The two items, the SPI and the authentication data are of special value. Firstly, the SPI that specifies which group of security protocols the sender is using. Secondly, the authentication data itself that is achieved by applying the algorithm stated in the SPI to the packet’s payload is used to authenticate the packet.
It is important to realise that AH does nothing to encrypt or in any way try to keep the data confidential. If an attacker were to intercept the packets with a network sniffer then the attacker would be able to read the contents of the package. This would however not enable the attacker to alter the contents of the package and resend it without generating a new hash value. AH also offers an anti-replay service that enables the receiver to help counter denial-of-service attack that would use retransmissions of the packets. Denial-of-service attacks are aimed to prevent or inhibit a normal use or management of communication facilities (Brown, 1999). The attack may be aimed particular destination, or it may be aimed to disrupt an entire network by overloading it, e.g. a web e-commerce site. To counter eavesdropping it is necessary to turn to encrypting the data with Encapsulated Security Payload (ESP).

The second part of the IPSec protocol suite, the ESP, is responsible for encrypting a packet. Just like the AH header the ESP is inserted into the IP packet between the IP header and the data. This is illustrated in Figure 3. ESP encrypts the data and thereby alters the payload content of the IP packet. Just as AH, the ESP contains SPI to indicate to the receiver what security measures have been taken by the sender to encrypt the contents of the packet. This allows the receiver to decode the package on arrival. There is a sequence number in the ESP header that increases each time a packet is sent to the same address during the same SPI. The sequence number indicates in which order the packets are supposed to be and how many packets have been sent within the same group of parameters. This provides protection against replay attacks. Where the attacker tries to send packets out of order to confuse the communicating nodes.
Before applying ESP

<table>
<thead>
<tr>
<th>Original IP header</th>
<th>TCP</th>
<th>DATA</th>
</tr>
</thead>
</table>

After applying ESP

<table>
<thead>
<tr>
<th>Original IP header</th>
<th>ESP header</th>
<th>TCP</th>
<th>DATA</th>
<th>ESP trailer</th>
<th>ESP authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Encrypted          |             |     |      |             |                   |
|                   |             |     |      |             |                   |
| Authenticated      |             |     |      |             |                   |

**Figure 3.** IP packets before and after applying ESP. Adapted from Kosiur (1998:99).

ESP can support a number of different encryption algorithms. It’s entirely up to the user to decide which algorithm to use. It is even possible to use different algorithms for different receivers. IPSec has the DES-CBC (DES with Cipher Block Chaining) as the default encryption algorithm. This ensures that a minimal interoperability exists between IPSec networks. Using DES-CBC algorithm requires a 56-bit DES secret key, which is included as a part of the security association. In order to use CBC, a 64-bit initialisation vector is required, and the data is processed in 64-bit blocks. The packets data is padded to create an integral number of 64-bit blocks if necessary.

ESP can also be configured for authentication. The ESP authentication field, which is optional in the header, contains a cryptographic checksum that is computed over the remaining part of the ESP (with the exception of the authentication field itself). This checksum varies in length due to the chosen authentication algorithm. Authentication can also be entirely skipped, if it is not necessary to authenticate the user.

It is important to remember that even though both ESP and AH can provide authentication, only ESP offers encryption of the data. Using ESP for both encryption and authentication reduces the amount of work needed to be done during packet processing instead of using ESP for encryption and AH for authentication. This is illustrated in Table 1.
Background

<table>
<thead>
<tr>
<th>Access control</th>
<th>AH</th>
<th>ESP (only encryption)</th>
<th>ESP (encryption + authentication)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectionless integrity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data origin authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Rejection of replayed packets</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Limited traffic flow confidentiality</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 1. AH and ESP comparison. Adapted from Stallings (1999:404).

The IPSec suite allows AH and ESP to be applied to an IP packet in two different ways, called modes (Stallings, 1999). These two modes are transport mode and tunnel mode. In transport mode only the transport layer segment of the IP datagram is processed (i.e. authenticated or encrypted). In tunnel mode, authentication and encryption is applied on the whole packet. This is illustrated in Figure 4.

![Diagram of transport and tunnel modes](image)

Figure 4. Transport and tunnel modes. Adapted from Kosiur (1998:103).

Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP packets. Transport mode operation can be described as follows. At the source of the packet, the block consisting of the ESP trailer plus the entire transport-layer segments is encrypted and the plaintext of this block is replaced with a cipher text to form the IP packet for transmission. Authentication is added if the optional authentication is selected. During the routing to the destination then each intermediate router examines the packet and processes the IP header plus any plain text in the IP packet. The router does not inspect any part of the cipher text. The destination node receives and examines the packet, processes the IP header plus any plain text in the IP packet. Then, based on the SPI in the ESP header, the destination node decrypts the remainder of the packet using the correct algorithm to convert the cipher text to plain text. The transport mode offers encryption for all applications that use IPSec with ESP. The drawback of using transport mode is that it is possible to do a traffic analysis on the transmitted packets. Thereby finding out the destination of the packet.
The tunnel mode ESP is used to encrypt an entire IP packet. The ESP header is prefixed to the package and then the packet and the ESP trailer are encrypted together. The entire block is encapsulated as seen in Figure 4 b), thereby hiding the destination address with cipher text. Then a new header that will contain sufficient information for routing but not for traffic analysis is added. This method is used to counter traffic analysis (Stallings, 1999).

Transport mode is suitable for protecting connections between hosts that support the ESP feature. On the other hand, tunnel mode is useful in configurations that include firewalls or some sort of security gateways. In the tunnel mode the only encryption that takes place is between an external host and the gateway or firewall, or between two gateways or two firewalls. After receiving the packet at the destination gateway the packet is decrypted and sent along on the local net to the designated receiver.

The IPSec suite offers secure communications across a LAN, across private and public WANs and the Internet. It is possible to connect branch offices with VPN over the Internet. This reduces the need for leased lines, which are expensive. IPSec offers secure remote access over the Internet for telecommuters and distance workers thereby reducing the cost for connection to the main office. IPSec can even be used to establish extranet and intranet connectivity between sites and other business partners.

Figure 5 illustrates the connection between main office, partner and telecommuter. The businesses maintain LANs at their offices. Non-secure IP traffic is on the LAN. If the traffic is headed out of the LAN then as the traffic passes a gateway it is encapsulated into a new packet with IPSec tags and encrypted. Incoming traffic is decrypted before it is allowed into the LAN. These operations of the gateway are transparent to the user and servers on the LAN. Telecommuters that want to connect to the office can dial to the Internet and with implemented IPSec protocols are able to connect to the office in a secure way.

![Figure 5: VPN illustration.](image-url)
Stallings (1999) states the following as the main properties of VPN:

- When IPSec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organisation.
- IPSec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper-layer software (including applications), is not affected.
- IPSec can be transparent to end-users. There is no need to train users on security mechanisms, issue keying material to each user, or revoke keying material when users leave the organisation.
- IPSec can provide security for individual users if needed. This is useful for telecommuters and for setting up a secure virtual sub-network within an organisation for sensitive applications.

2.1.2 VPN with PPTP

A PPTP VPN is less complicated, with less options and protection than the IPSec VPN. With the support of PPTP in Windows NT Server the protocol has become very popular and is implemented by many Internet Service Providers (ISP). The PPTP along with Layer 2 Forwarding (L2F) from Cisco will build the Layer 2 Tunnelling protocol (L2TP) that will eventually replace the L2F and the PPTP protocols. The PPTP protocol was created by the PPTP forum, which includes 3Com, Microsoft, US Robotics and others (Kosiur, 1998). The basic idea was to use the Internet’s infrastructure to provide secure connection between networks and clients. Remote users would dial to the local ISP and could then connect to the corporate network safely and securely.

The most common way to connect to the Internet with a dial-up connection is by using the Point-to-Point Protocol (PPP). PPTP uses the functionality of the PPP to provide a dial-up access to the ISP that would then tunnel the packets to the destination address. The current implementation of the PPTP protocol specifies that PPTP encapsulate PPP packets using a modified version of the Generic Routing Encapsulation (GRE) protocol. GRE gives the PPTP the flexibility of handling protocols other than IP, such as IPX and NetBEUI (Kosiur, 1998).

PPTP uses the authentication mechanisms that are included in PPP, namely Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Microsoft has introduced a new version of CHAP, MS-CHAP that is the result of the strong connection between PPTP and Windows NT. CHAP utilises information that is found within NT domains for security. Bruce Schneider¹, Mudge

and L0pht Heavy Industries released an analysis of Microsoft PPTP and found serious security flaws in the MS-CHAP, which has resulted in the creation of a new version of MS-CHAP, namely MS-CHAPv2. PPTP uses PPP to encrypt data. The improvements from CHAPv1 to CHAPv2 include longer keys, improved algorithms to derive keys and confirmation from server. Microsoft has even developed a stronger version of the encryption algorithm, called Microsoft Point-to-Point Encryption (MPPE), this algorithm prevents trivial cryptanalytic attack of XORing the text stream to crack the encryption by using different keys in each direction.

Both PAP and CHAP rely on safe storage of a secret password on the end user computer and the server computer. If the security of either computer is jeopardised and a risk is that the password has fallen into the hands of a cracker then both passwords must be changed. It is also a problem that end user receives access privileges assigned to the DTE. This implies that two different users cannot share the same DTE with different privileges to access different files or folders.

The PPTP architecture consists mainly of three things, firstly the connection and communication, secondly the control connection and thirdly the data tunnelling. The connection and communication is used by a PPTP client to establish a PPP connection to an ISP either through an ordinary Public Switched Telephone Network (PSTN) line or by Integrated Services Digital Network (ISDN). Using that PPP connection the client establishes a control connection with the PPTP protocol from the client PPTP to the PPTP server. This connection is called tunnel and is accomplished by using Transmission Control Protocol (TCP) to establish the connection. The data tunnelling is accomplished by using the PPTP to create encrypted PPP packets that are then sent through the tunnel on the Internet to the PPTP server. Once the packet arrives at the PPTP server, the packet is disassembled and decrypted and then the decrypted PPP packets are sent to the receiving computer on the local network.

The PPP is a remote access protocol used by PPTP to encapsulate the different protocol packets such as IP, IPX and NetBEUI to be able to send them over a TCP/IP connection. The PPP establishes and ends the connection to the ISP and between the remote computers. The PPP allows for authentication with clear text or encrypted messages. The PPP creates TCP/IP packets that can contain other protocols than TCP/IP; an example of a TCP/IP connection is a direct connection to a TCP/IP network that is remote from the corporate network. These packets are encrypted before they are sent to their destination. It is important to remember that the packets are encrypted from the PPTP client computer to the PPTP server on the corporate LAN.

Control messages are used to establish, maintain and end PPTP sessions. The control messages are sent as a TCP datagram between the server and the client, if the client is not PPTP enabled then the control messages are only transmitted between the PPTP server and the ISP server. Control packets are periodically sent to inquire about link status and to send control information between the endpoints in the tunnel. The data connection that is established uses the Generic Routing Encapsulation (GRE) to create the IP datagrams that are sent between the client and server. The encapsulated payload is actually the PPP packet data. This is illustrated in Figure 6. The GRE header actually encapsulates the PPP packet within the IP datagram. The GRE protocol
contains information on the host’s call ID, which is used to monitor transmission rate and acknowledgement capability.

<table>
<thead>
<tr>
<th>Media</th>
<th>IP</th>
<th>GRE</th>
<th>PPP</th>
<th>PPP Payload</th>
</tr>
</thead>
</table>

**Figure 6.** IP-datagram. Adapted from Kosiur (1998:127).

There are various tunnel types available today, which allow for different types of connections based on the capabilities of the end user and the ISP. It is up to the end users computer to decide where the termination point of the tunnel is, either at the ISP’s computer or at the end user computer. There are however mainly two types of tunnels that are widespread. Those are voluntary tunnels, seen in Figure 7; these tunnels are set up at the request of the end user and allow the end user to simultaneously use other services on the Internet. Voluntary tunnels provide both privacy and data integrity for Intranet traffic that is sent over the Internet. Compulsory tunnels on the other hand can be transparent to the end user as they are created automatically without any action on the end users behalf. Compulsory tunnels offer better way to control access to the corporate network than voluntary tunnels. Compulsory tunnels can also allow the corporation to exclude Internet, while still allowing the employee to connect to the corporate network. Another benefit of the compulsory tunnel is that the tunnel has predetermined endpoints and multiple client connections can be carried over the Internet in the tunnel, thereby reducing the amount of bandwidth needed to transport the information over the Internet. The disadvantage of a compulsory tunnel is that no encryption is applied outside the tunnel, i.e. between the Remote Access Service (RAS) and the end user. A compulsory tunnel can be seen in Figure 7.
Dial-in VPNs have become very popular because the PPTP is included in the windows operating systems Windows 98 and Windows NT. Even though a standard body like the Internet Engineering Task Force (IETF) has not ratified the PPTP it is very popular and widespread thanks to Microsoft. Dial-in was the original focus of the PPTP with no support for LAN-to-LAN tunnels.

LAN-to-LAN tunnels were not supported within PPTP until Microsoft introduced Routing and RAS for NT servers. LAN-to-LAN tunnelling occurs between two PPTP servers and thereby connecting two different LANs. The PPTP architecture does not make use of key management system and therefore all authentication and encryption is managed with CHAP or MS-CHAP. To create a LAN-to-LAN connection one of
the PPTP servers will act as a PPTP client while the other server will act as a PPTP server. A LAN-to-LAN tunnelling that occurs between two PPTP servers work much like IPSec security gateway that connects LANs.

The main advantages of the PPTP is that it runs on the data link layer or layer 2 of the OSI model as opposed to IPSec, which runs on, layer three. This enables PPTP to run more than just the IP protocol over its tunnels, while IPSec only can send the IP protocol through its tunnels. Another significant difference between IPSec and PPTP is that PPTP allows for outsourcing of some functions to a local ISP, i.e. it is possible to let the end user dial-in to the ISP instead of having to set up a local connection points. At a corporate site the PPTP server acts in a similar way as IPSec security gateway, the PPTP client acts similarly to the IPSec client with the exception of key exchange. This is illustrated in Figure 8.

![Figure 8. The difference between IPSec and PPTP. Adapted from Kosiur (1998:136).](image)

The most recent addition to the VPN protocol suites is the Layer 2 Tunnelling Protocol (L2TP). The L2TP protocol is based on the Layer 2 Forwarding from Cisco Systems, which is to be compared to the PPTP standard from Microsoft. L2TP is Cisco’s solution on the tunnelling through the Internet. L2TP has evolved from those two standards that are supported by both Cisco and the Microsoft group. Just like PPTP and L2F, L2TP is an extension of the PPP.
The key benefits of the L2TP protocol suite are that it offers hiding of the so-called attribute value pair, where attribute is “user” and value “john”. Perhaps the most important change is the interoperability between vendors. This allows for the use of third party software and hardware in a VPN solution where L2TP is used as the protocol suite.
3 Problem description

Information exchange between business partners, from branch office to main office and from distance workers to the office can provide valuable information, which can aid in the survival of the company. The limitation of today’s computers is much less than what it was only couple of years ago. With a 56k modem, it is not likely that the end user will notice any reduction in the throughput when he changes from a regular connection to the ISP to an encrypted VPN tunnel. The reason is that software based encryptions can encrypt more data than can be sent with the bandwidth available on modems. Users that have a leased line with smaller capacities may not notice any reduction in speed even though they are using software based encryption. This is because leased lines are often low speed lines, i.e. low bandwidth, and the computer will be able to encrypt more than the line can carry. When a change is made from a regular leased line to a point-to-point connection with VPN through the Internet the need for more powerful encryption may arise with more bandwidth, which would then be a hardware based encryption system because of the higher encryption speed.

The change toward VPN is mainly driven to save money on expensive leased lines and the possibility to let mobile workers access the companies’ main computers, while on the road. Or as Rich Tong, division marketing manager of the business systems division at Microsoft said:\footnote{Tong, R., 1996, \textit{Microsoft Leads Initiative for Virtual Private Networks Across the Internet}, [online]. Available from: http://www.microsoft.com/PressPass/press/1996/mar96/pptppr.asp [Accessed May 17th 2000]}

"Point-to-point tunnelling protocol gives users an easy, low-cost and secure way to extend a private network across the Internet"

One can easily argue that easy should apply to the whole solution and not only a part of it, therefore it should mean that the protocol is both easy to install and to administer.

3.1 Yesterday’s Internet

Until recently Internet did not allow companies to transmit classified information over the Internet safely and securely, instead the companies had to rely on leased lines and telephone calls, sometimes long distance, to be able to send classified information between two points. By leasing lines, companies are trying to safeguard against eavesdropping but it is important to keep in mind that it is very easy to eavesdrop even on telephone lines today. Branch offices can use modems or gateways to establish contact with the companies’ main computer or to use a leased line from point A to point B, sometimes across the country. This is illustrated in Figure 9.
Problem description

![Diagram](image)

**Figure 9.** Leased line and direct call to main office. Adapted from Kosiur (1998:118).

This solution works well for smaller companies that work in the same geographical area and thereby avoid the cost of long distance calls to connect to the main office. However, as companies expand to new geographical areas this solution becomes impractical and expensive. This is because long distance phone calls are not cheap; in fact, telephone calls can be quite expensive if they are made from outside the country. With increased number of offices, it is easier to let a local ISP take care of the trouble of connecting the branch office to the main office through the Internet.

This leads to new solutions to interconnect offices, namely VPN, where the remote office, main office and the mobile user connect to the Internet locally, either through a permanent connection or by using an Internet Service Provider (ISP) that supports VPN standard such as PPTP. This is illustrated in Figure 10.

![Diagram](image)

**Figure 10.** VPN with the aid of the Internet. Adapted from Kosiur (1998:118).

By utilising the Internet as a bearer of information between two points, the issues of security, integrity and authentication are solved by using some of the VPN protocol suites. With the main servers all located in the same spot, all administration, backup
and other administrative duties are in the same location, thus making it easier to administer the servers. This also aids in reducing costs for administration.

To reduce costs companies may want to be able to send sensitive information by using the Internet as a transport medium anywhere in the world. This could be sensitive business information or even surgery video feed that could reveal the patients identity or contain patient info. The information is often extremely sensitive and needs as much protection as can be provided. Information that concern business secrets or patient data can be worth a lot to hackers that could use the information in a malicious purpose to blackmail the owners of the information.

With the VPN technology, it is possible to use the Internet as a carrier of such sensitive information. The main question is the security of transferring the sensitive information between two points. How is that done in a manner that is acceptable from a security standpoint? It can be achieved by using cryptography to encrypt the data that is to be sent with standard encryption algorithms such as DES and Triple-DES and others algorithms that have previously been named.

3.2 Tomorrow’s Internet

When companies protect their servers and other computers, with a firewall, it implies that their employees cannot access the company servers that are behind a firewall, and that a remote office site is not allowed to access the servers behind the firewall due to the risk that separate IP addresses make up a weak point in the system that allows IP-spoofing. IP-spoofing is where the attacker assumes the identity of a third party to gain access to the system (Brown, 1999). With the right restrictions, an administrator can reduce the risk for IP-spoofing and only allow previously accepted IP addresses to pass through the firewall. For some companies the solutions are costly leased lines, which safely can access the companies’ servers and for others the solution is VPN. The question is what method is the best with respect to speed, safety and reliability.

Faster and more powerful computers contribute to the fact that it is no longer the computers that are the limiting factor, but the bandwidth that is used to connect computers to the Internet. According to Andersson (1999) the computers are able to encrypt 0.5Mbit of data per second by using a software encryption system. This is not a problem with a 56Kbit line or with 64/128Kbit ISDN; the problem is when a larger connection such as 10Mbit Ethernet connection is used. That is, only transparent gateways that are software based would create a delay in transmission because they can only send about 0.5Mbit per second. If a chip based encryption system would be used the encryption speed would rise to about 100Mbit per second (Andersson, 1999). This is sufficient to encrypt video feed, for an example a surgery or digital roentgen pictures.

Due to enormous costs of a hardware based encryption system today, with prices ranging from $10,000 and upwards it is not possible to fit every notebook with a hardware based encryption. It is not necessary because of the limited bandwidth that is available by modem. A hardware based encryption system is better suited at gateways and routers where large amounts of traffic pass through rather, then at someone’s home with a single laptop. The need for bandwidth of different applications can be seen in Figure 11. The bandwidth differences show that some applications can use software-based encryption, while others such as medical
imaging, would need hardware based encryption to work with optimal performance while for speech it would suffice with software-based encryption. Medical images are often a much larger file that would take long time to encrypt and send. Speech files are often smaller and therefore can it be easier to encrypt and send speech files than image files.

![Diagram of Bandwidth Requirements](image)

**Figure 11.** Bandwidth requirements of file types. Adapted from Kosiur (1998:170).

In theory VPNs are relatively easy to use, once the VPN has been set up. The end-user uses transparent VPNs, i.e. the users are not aware of the VPN program that is performing the encryption and decryption on the user’s computer. This contributes to the safety in a way that the user doesn’t have to turn on the VPN functions. They are automatically turned on and encrypt and decrypt the traffic passing to and from the end-user computer. VPNs contribute to safety by encrypting all traffic that is sent between two computers. This is accomplished by using various types of algorithms and protocols, such as IPSec and PPTP. With increased key length, it is becoming increasingly difficult to crack a packet that has been encrypted. With a key length that is 56 bits there are $2^{56}$ possible keys available, which corresponds to approximately $7.2 \times 10^{16}$ keys. By just adding one bit to the encryption key, i.e. 57 bits, the possible
keys are approximately $2^{57}$; they therefore double to approximately $1.44\times10^{17}$ keys. This explains why larger keys take longer time to crack with a brute force attack. Today it is possible to achieve up to 168-bit encryption with approximately $3.74\times10^{19}$ keys, which would take millions of years to crack with today’s technology (Stallings, 1999). The most common encryption outside the USA is, however, the 56-bit encryption. This is due to the export restrictions set by the U.S. government. This is changing, however, and 128-bit encryption is becoming increasingly common as the U.S. government eases on its encryption export restrictions. Asymmetric keys need to be much bigger to provide the same protection as symmetric keys. A 128-bits symmetric key (private key) would have to be 2,304 bits as an asymmetric key (public key) to provide the same protection from a brute force attack (Kosuri, 1998). The asymmetric keys are longer due to different mathematical algorithms. An estimate of the time needed to crack different symmetric keys and the estimated cost of the equipment needed to break it in 1998 is illustrated in Table 2.

<table>
<thead>
<tr>
<th>Cost</th>
<th>40</th>
<th>56</th>
<th>64</th>
<th>80</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>$100k</td>
<td>2 seconds</td>
<td>35 hours</td>
<td>1 year</td>
<td>70,000 years</td>
<td>$10^{10}$ years</td>
</tr>
<tr>
<td>$1 million</td>
<td>0.2 seconds</td>
<td>3.5 hours</td>
<td>37 days</td>
<td>7000 years</td>
<td>$10^{18}$ years</td>
</tr>
<tr>
<td>$100 million</td>
<td>2 milliseconds</td>
<td>2 minutes</td>
<td>9 hours</td>
<td>70 years</td>
<td>$10^{16}$ years</td>
</tr>
<tr>
<td>$1 billion</td>
<td>0.2 milliseconds</td>
<td>13 seconds</td>
<td>1 hour</td>
<td>7 years</td>
<td>$10^{15}$ years</td>
</tr>
<tr>
<td>$100 billion</td>
<td>2 microseconds</td>
<td>0.1 second</td>
<td>32 seconds</td>
<td>24 days</td>
<td>$10^{13}$ years</td>
</tr>
</tbody>
</table>


By deciding to use a VPN as part of a corporate network, companies are making a bit of a gamble. Companies are really at the mercy of the ISP that delivers the VPN solution. There is no way that the company can influence or affect the ISP in any way to minimise down time. This is perhaps the biggest drawback of a VPN, i.e. not being able to control the availability of the connection oneself but having to rely on a third party to provide the connection. This can be solved to some extent by setting up own access points but that would reduce the benefits of setting up a VPN. In today’s market-based economy a failure is not acceptable from the clients viewpoint. Therefore, the ISP’s are very anxious to deliver top service to companies. The conclusion is that it is very unlikely that an ISP would fail to give the requested service to the buyer; so even if a company lays the responsibility of the connection on an ISP it can be relatively certain that the chance of something not working is remotely small.

3.3 IPSec and PPTP VPNs

The two different protocols, i.e. IPSec and PPTP, that have previously been introduced share some functions and aspects and differ in others. The reason for the choice of IPSec and PPTP is that these two protocol work on a different level of the OSI model seen in chapter 2. IPSec works at layer 3, while PPTP works at layer 2. Both have benefits and drawbacks depending on which layer the protocol is working at. The speed of the encryption is among other things based on which layer the encryption is done and on what kind of encryption algorithm used.
The aim of this work is to analyse the two protocols PPTP and IPSec that are most widespread on the VPN market. There are several things that will be evaluated during the analysis of the protocols. The installation of the two protocols and the complicity of getting the protocols up and running. That is to install the protocols and to see if the function properly from start. Another aim is to see if the PPTP and the IPSec protocols can acquire the same encryption speed with software based encryption solution over different bandwidths and with several different file types. If the two protocols differ in speed, which algorithm is the one that provides better, faster encryption and a better security? The third aim is to analyse the difference of the security aspects of the two protocols with respect to key sizes, ease of cracking and encryption strength.

Both protocols belong to the VPN suite. The VPN suite is a collection of protocols that utilise the Internet for safe transport of data between two endpoints. These two protocols offer two different approaches to the encryption problem. They use two different layers of the OSI model and are simply very different.

The interesting thing is to see if the two protocols differ in installation work, if the manuals are adequately well written to allow for easy installation. Finally to examine if there are any suggestions as to what to do if any troubles occur with the installation of the two protocols.

As was explained earlier in this chapter, Microsoft’s press releases can be interpreted as claiming that the protocol should be easy to install and administer. The software that is needed is already built in the operative system and should therefore be easy to install. This claim will be tested in the installation phase. Microsoft also claims that administration of the equipment is easy. Therefore during the installation phase an evaluation of the PPTP protocol should be conducted to verify that the administration is as easy as they claim.

Of particular interest would be to see if the two protocols differ in encryption speed and to see if software based encryption can encrypt more than what the available bandwidth could carry. Would the user notice any difference in transfer rate depending on what file type is transferred or the frame size of the packets that are being transferred? However, measurements of the transmission speeds are not done in this project, but left for future work.

Other, more technically resource demanding solutions that involve advanced equipment, more equipment and multiple users at the same time would of course be preferred, but at this time it is impossible to acquire the equipment and the time allocated for the project is too narrow to complete the trials of such an advanced experiment.
4 Methods

As previously described in chapter 3 the protocols will be installed on the computers
to evaluate the installation phase of the protocols that are to be tested. A literature
search will be done, in order to find if there are any experimental studies of
transmission speeds of the two protocols. Finally an analysis of the security
perspectives of the two protocols will be done, focusing on the strengths and
vulnerabilities of the two protocols.

There are several ways to evaluate VPN solutions; among those are various technical
experiments and literature studies. There is always a risk that the papers, articles and
books that a literature study is based on may have become obsolete due to rapid
development in the field of data communications. The security analysis will be based
on a literature study to give insight in the security aspects of the protocols based on
the solutions available today. The objectives of this project are to examine
transmission speed, bandwidth and security aspects of two protocols within the VPN
architecture.

4.1 Evaluating installation and encryption

This chapter describes a proposed architecture for testing the protocols. The speed
tests have not been conducted in this project because of the problems with the
installation, as described in chapter 5 and will therefore be based on a literature study.

This architecture could be used for testing the installation procedure, encryption and
transmission speeds. There are several different ways to design a VPN solution that
reflects the real world but it is important to keep in mind that a simple solution does
not carry as many options and possible complications as a complicated solution
would. It is therefore beneficial to choose a solution that is as simple as possible to
solve this project and at the same time gives realistic view on the test phase. Many
factors affect the results of a project like this and all efforts should be made to keep
the factors that can affect the project as few as possible.

The simulation setup gives an idea of how it is to install a VPN solution in a real
world environment. With the manuals to the protocols and the positive comments
from the producers of the programs about how easy it is to install the protocols, it
should not be any problem to install the protocols. This should be done to verify that
the installation procedure goes as smooth as the installation instructions that came
with the PPTP and IPSec protocols indicate.

The simulation environment represents a possible combination of a corporation,
where a server is connected to both a local LAN and a mobile user or remote office
through modem connection. It covers many aspects of a real life situation but not all
aspects, for example, a leased line connection to a partner where two gateways are
involved or multiple servers, communicating between two different computer
segments within a company through multiple gateways or multiple servers are not
represented.
In the test, a collection of 3 clients was to be used to simulate calling client, a client on LAN and a server. A measure of the throughput between the clients and the server should have been made, both with calling client, using a 56Kbit/sec modem to server scenario and a LAN client to server scenario. This was not done due to problems with the installation of the protocols. In selection of the architecture, the aim was to simulate situations that could occur at companies. Full test should have been done both with the modem connection and with the LAN connection with both protocols and various file types that may be encountered in everyday transmissions, but that was not done due to installation problems that are explained in chapter 5.

The first tests should be conducted in a LAN environment that includes a connection of a Windows 98 client to a Windows NT 4.0 server with SP6. Then the same scenario will be repeated only that the connection should be through a modem instead of LAN. This is illustrated in Figure 12.

**Figure 12.** The test lab setup.

The main aim is to see if encrypting various file types takes longer time to perform and send than other and to see if a video feed is possible with software encryption. Another aim is to see if the frame size of the packets matters in encrypted transmissions. The netXray program can generate traffic that is set in different sized frames and then sent away to the receiver. The netXray program would have to be on the server or the client to be able to generate traffic that would be encrypted according to the PPTP or the IPSec protocols.

All the tests should be run three times and a mean average value should be calculated from those three tests. The results should be presented in a table that shows how much data was been sent over what connection and how long time it took to send it.

The file types that should be used represent a broad spectrum of the Internet traffic today. The most complicated file structure is the streaming video with sound. This file type places high demands on the bandwidth and it will certainly fail over a 56Kbit modem. The second file type was a digital medical image, a roentgen picture on a digital form. This file does not place as high demand on the bandwidth nor will the last two file types do that. The last two file types that should be used send a sound file and a text file through a the VPN connection.
The hardware that was used during the installation phase is presented in Table 3.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 clients</td>
<td>Each client has a 166 MHz MMX Intel processor; 32 Mb RAM, an Intel 10/100 Mbps Ethernet card built into the motherboard and Windows NT Workstation operating system with Service Pack 6a (SP6a) installed.</td>
</tr>
<tr>
<td>Server</td>
<td>The server has a 166 MHz MMX Intel processor; 64 Mb RAM, an Intel 10/100 Mbps Ethernet card for local connection, a 3Com 10/100 Ethernet adapter for connection to the modem pool server and Windows NT 4.0 with SP6a operating system.</td>
</tr>
<tr>
<td>Measurement computer</td>
<td>The measurement computer is a Dell Cpi, 450 MHz computer with 128 Mb RAM and 3Com 10/100 Ethernet card.</td>
</tr>
<tr>
<td>2 hubs</td>
<td>The hubs are Bay Networks, Netgear 10 Mbps 8-port hub with uplink option (Netgear TP-108).</td>
</tr>
<tr>
<td>Media</td>
<td>The computers are connected with UTP CAT 5 cables on the LAN and with serial cable to the modem.</td>
</tr>
<tr>
<td>Modem</td>
<td>3Com/U.S. Robotics 56 K analogue faxmodem.</td>
</tr>
</tbody>
</table>

Table 3. The hardware used.

4.2 Evaluating security

The security evaluation is mainly based on a literature study from Brown (1999) and Kosiur (1998), because they present the security aspects of these two protocols clearly in their books. White papers could give more updated information about the security of the protocols but the information could be more difficult to summarize. The previously named books will be used to summarize the security aspects of the two protocols.

Physical testing of the security aspects of the two protocols takes long time and demands much knowledge of the protocols and advanced equipment to crack the keys. The knowledge of the security aspects are presumed to be inadequate to perform physical tests of the protocols and the time needed to acquire the knowledge is assumed to be to short. The equipment that would be required to mount a serious security attack against one of the protocols is also not available.

A literature study presents the benefits and the drawbacks of each protocol in a clear and concise manner. The protocols will be analysed on three points, which are:

1. Strength
2. Vulnerability
3. Attack types

These three points represent the main issues of the security aspects of the PPTP and IPSec protocols. This allows for easy evaluation of the protocols based on the strengths and the vulnerabilities of the two protocols.
5 Analysis

Analyses of the results from the installation of the test lab are presented in this chapter. An evaluation of the transmission speeds of the IPSec protocol is then presented and finally a comparison of the security aspects of PPTP and IPSec is presented.

5.1 The installation phase

The purpose of the installation phase was to setup the test lab according to the vendors’ instructions and to see if it really was as easy as they claimed. The trials of the two protocols did not go as expected. The PPTP protocol did not work as planned and was finally abandoned in favour for the IPSec protocol, the causes can be seen in 5.1.1 The PPTP trial. The testing of the IPSec was somewhat more successful than PPTP but it did not however function satisfactory, the results are presented in chapter 5.2.1 The IPSec trial.

5.1.1 The PPTP trial

The trial of the PPTP protocol suite by Microsoft was first. The computers were set up and tested to see if they were able to establish contact by pinging each other. When the contact had been verified the computers were set up to handle the PPTP protocol with Remote Access Service (RAS), thereby enabling dial up networking (DUN). All set ups were done according to Microsoft’s own white paper on PPTP\(^5\). Even though that every recommendation was followed in the white paper and then double-checked the connection did not work.

The white paper from Microsoft had detailed instructions on how to set the protocol up, but lacked information on troubleshooting the protocol. This can be seen here where the white paper “Implementing MS PPTP” in detail describes how to set up the client:

To install the PPTP protocol on a PPTP client running Windows NT
Workstation version 4.0 or Windows NT Server version 4.0:

1. Click Start, point to Settings, and then click Control Panel.
2. In Control Panel, double-click Network.
3. Click the Protocols tab, and then click Add to display the Select Network Protocol dialog box, shown in Figure 7.
4. Select Point To Point Tunneling Protocol and click OK.
5. Type the drive and directory location of your installation files in the Windows NT Setup dialog box, and then click Continue. The PPTP files are copied from the installation directory and the PPTP Configuration dialog box will appear as shown in Figure 8.
6. Click the Number of Virtual Private Networks drop-down arrow and select the number of VPN devices you want the client to support. You can select a number between 1 and 256 for computers running Windows NT Workstation version 4.0 or Windows NT Server version 4.0. Typically, only one VPN is installed on a PPTP client.

\(^5\) Microsoft, 1998, Implementing MS PPTP, White paper, Microsoft Inc., Seattle, USA.
Analysis

Note If the PPTP client is an ISP server running Windows NT Server version 4.0, you can select multiple VNP devices as needed to simultaneously support the PPP clients using the ISP server to connect to a PPTP server. Windows NT Server version 4.0 supports a maximum number of 256 VPN devices.

7. Click OK, and then click OK in the Setup Message dialog box.
8. In the Remote Access Setup properties dialog box, you can do either of the following:
   a) Temporarily stop installation of PPTP by clicking Cancel, closing Network, and then shutting down and restarting the computer. Note that you must perform the procedure described in the following section "Adding a VPN Device as a RAS Port on the PPTP Client" to complete installation of PPTP.
   b) Continue installation by clicking Add to add to RAS the VPN device installed with PPTP. (See step 5 of the procedure described in the following section.)

But as the content list of the Microsoft white paper shows there is no section on troubleshooting or where to seek for further assistance on the installation of the PPTP protocol in case of problems:

Contents
Using PPTP
Planning for PPTP and Virtual Private Networks
Hardware Requirements
Network Protocols on the Private Enterprise Network
Before Installing PPTP
Installing and Configuring PPTP on a PPTP Server
Installing PPTP on a PPTP Server
Adding VPN Devices as RAS Ports on a PPTP Server
Configuring PPTP Server Encryption and Authentication Options
Configuring Server Encryption for PPTP
Configuring PPTP Filtering on the PPTP Server
Configuring LAN Routing on the PPTP Server
Installing and Configuring PPTP on a PPTP Client
Installing PPTP on a PPTP Client
Adding a VPN Device as a RAS Port on the PPTP Client
Configuring Dial-Up Networking on the PPTP Client
Creating the Phonebook Entry to Dial an ISP
Creating the Phonebook Entry to Dial a PPTP Server
Using PPTP to Connect to a PPTP Server by Dialing An ISP
Dialing-Up an ISP PPTP Service to Connect at a PPTP Server
Using PPTP Over the LAN to Connect to a PPTP Server

The first part of the experiment went as planned, the lab was setup and client on the LAN was able to ping the server and vice versa. The computer with the modem was then setup and called the modem-pool and when it was connected with the modem-pool server it was able to ping the PPTP server and vice versa. The conclusion is that all communications medium functioned properly. Once the PPTP protocol was turned on, the clients and the server, everything stopped working and multiple failure messages appeared on the clients. As soon as the PPTP had been setup it was no
longer possible to ping the server, neither from the client on the LAN nor from the client on the modem connection. This led to a search for what was wrong with the lab environment.

An extensive failure search was then initiated to find out what had been done wrong. First, a thorough inspection of the TCP/IP protocol was performed to ensure that it was possible to ping all the computers that were supposed to be reached during the test. This succeeded sometimes and failed at other times. When the pinging failed it was necessary to remove the TCP/IP protocol from the server and then to reinstall the TCP/IP protocol to enable the server to be reached by all participating computers. This occurred several times during the PPTP trials.

- **Error 741. The local computer does not support encryption**
  The computer with the modem connection was tested for functionality with the server with no encryption installed. It worked well, but as soon as the encryption was applied, it was not possible to reach the server. It was possible to ping the server but it was impossible to establish a VPN connection to it.

- **Error 742. The remote computer does not support encryption**
  The computer on the LAN was tested for functionality with the server with no encryption installed. It worked as planned; it was possible to ping both ways. However, as soon as encryptions were turned on it was not possible to establish a connection between the client and the server.

- **Error 629. The port was disconnected by the remote computer**
  As the client and server tried to negotiate on the password and key structure for the VPN connection a problem was discovered. The server would disconnect the client while the computers made the handshake. The explanation was that the line quality was bad or that there was a disturbance on the line that caused the computer to drop the connection. A possible cause to the problem could also be that the encryption level of the computers differed from each other. The encryption levels of the computers were the same throughout the tests except when they were specifically tested so.

**Encryption level modifications**
If a change were made with the clients to lower the encryption level, then the server would not answer the clients when they tried to call the server. Even if the encryption level of the server and the clients were lowered and kept on the same level, the server would either not answer when the clients called, due to the fact that the IP stack needed to be reinstalled as explained previously, or the connection would be dropped after handshake and password change. The dropping of the connection resulted in the appearance of error code 629.

A search for the cause of the failures and the solutions to them are presented as follows:

1. **Error 741 and 742.** Same setup on LAN and modem clients. Both the modem client and the LAN clients had exactly the same setup on the DUN. Even if they had the same setup the clients got different failure messages. No
explanation was found of what this could depend on, neither on Microsoft’s web site nor in the help files.

2. **Error 629.** The explanation for error 629 was found on Microsoft’s web page and in the help files of the operating system suggested that the line quality was bad or that some disturbance was on the line. The final suggestion was that the client and the server did not use the same encryption level. The line quality was a 10 Mbps Ethernet connection via hub directly to the server, during measurements it showed no interference on the line. Both the client and the server were set to use the same encryption level and handshaking while negotiating the protocol to use.

3. An attempt to modify the encryption level on the server resulted in the loss of connection to the world, i.e. it was no longer possible to ping the server or to ping anything from the server. The server had to have the TCP/IP connection removed and reinstalled for it to work again. This behaviour would repeatedly occur when something had been done that had to do with the PAP/CHAP selection of the PPTP protocol.

Despite an extensive search for the failure by more than one person, the solution to the problem of inoperability of the PPTP protocol was not found. To prevent that some basic failure had been made, the whole test lab was taken down and then the hard disks were formatted and a fresh versions of the operating system were put in again on the computers. The white paper on the MS PPTP installation was followed again. The results were the same as previously. It was not possible to establish a connection to the server with VPN. To rule out that the network cards were defect they were switched in the server in such a way that the network card that was supposed to be used on the local network was used on the external network and vice versa.

To be on the safe side a test was also made with the Windows 98 operating system on the clients. The Windows 98 operating system gave the same results as the previous tests with the Windows NT Workstation operating system. The same problems surfaced with the same error codes as before.

A search through the newsgroups available on the Internet revealed that several dozen individuals and corporations had problems with the PPTP installation. Lennart Nielsen at Uni-systems⁴ claims that he has also had problems with the Microsoft PPTP solution. Where he managed to establish contact but could only send and receive messages at 9600 bps. So others have also had problems with the configuration and installation of the PPTP system from Microsoft. Gary Davis, Information System Specialist at the American Cancer Society⁵ said that he had serious problems connecting the client to the server, where the server would kick the client out after 30 seconds of connectivity.

---

⁴ Nielsen, L., 2000, Re:VPN problems, E-mail to the author, June 8th 2000
⁵ Davis, G. 2000, May 27th, PPTP from 98SE to NT4sp6a problems! HELP!, [online], Available from: newsgroup: comp.dcom.vpn [Accessed June 12th 2000]
Microsoft has confirmed⁶ that a possible cause to the problem is that a problem exists with the DUN in the RAS service; this is due to the inability of the client to use the correct hashing to encrypt the password that is sent to the server while a 128-bit encryption is being used. Until recently the export restrictions on encryption from USA has been very strict. January 14th 2000, the US government eased its restrictions and allowed for 128-bit encryption to be exported¹. This has however not been implemented in all software yet and the software vendors have not yet implemented the eased restriction in their programs intended for the world market nor have they updated their web pages accordingly to allow for demo versions of their programs that support 128-bit encryption outside of the USA.

5.1.2 The IPSec trial

The IPSec protocol was tested after the PPTP protocol trial. The trial of the IPSec protocol did not go as expected due to several different reasons that are listed later. The CD with the program had detailed installation instructions that were followed exactly to ensure that the setup was performed correctly according to the supplier of the program.

The lab was set up with one client on a LAN connected to a server and another client on a modem connection to the server. The setup of the lab went as planned and the client on the LAN was able to ping the server and vice versa. The client that was connected through the modem pool had no problem to connect to the IPSec server, which was verified by pinging the server. When the installation of the IPSec program from F-Secure was initiated, the problems began. These problems were though different than the previous problems, meaning that the connection between the clients and the server were never lost, but it was impossible to establish an IPSec connection between the clients and the server.

When the first installation of the F-Secure manager server program was done on the server, a failure message appeared "Setup failed to write settings to the MS-IIS". It is unknown if this in any way affected the function of the F-Secure VPN+, during the trials it did not shown any failure messages that could be related to this message.

When the server installation was performed on the server the rest of the network disappeared, i.e. the client that was supposed to be on the local net disappeared. While the server is visible from the client, it is not possible to browse the server catalogues from the client side. As soon as the client had been created in the server policy domain template it was possible to browse the catalogues of the server.

The client/server communication did not occur through the IPSec protocol. In spite of repeating the installation procedure according to the installation manual for the F-Secure program a communication link with the IPSec protocol was not established. Research in the manual showed that the test lab was extremely low on resources as the


minimum requirements to run the IPSec management program was 64 Mb in memory. The clients only had 32 Mb of memory to work with. It was unclear in the instruction papers from F-Secure if there was a need for the management programs on the client side to require 64 Mb of memory or less. This was not perceived to be a problem with the lab as early research indicated that the F-Secure VPN solution had been commercial since 1996, indicating that system requirements would be rather low.

This lack of memory caused some error messages such as low on memory and low on virtual memory, when the F-Secure IPSec program was setup on the client computers. It was difficult to acquire more resources to the test lab; thereby it was difficult to avoid the memory failure messages that appeared from time to time.

The installation instructions for F-Secure were detailed but incomplete. As can be seen in this excerpt from the IPSec manual from F-Secure8:

When you have installed F-Secure Management Server and F-Secure Management Tools, run the F-Secure VPN+ installation and use either centralized management or a configuration disk prepared for each client, server, and gateway host. Centralized management is the recommended installation method.

Installing With Centralized Management
The workstation setup process allows the user to install the required software components from the CD-ROM. The administrator must have the administrator public key file (Admin.pub) available, either on a prepared configuration floppy disk or on a shared NT drive. You can get the admin.pub file from the root of the Management Server’s cmdir directory. This key is generated when F-Secure Administrator is run for the first time.

Running the Installation
The InstallShield Wizard will guide you through the setup. Click Next to continue.

Read the Important Information screen and click Next. Type your CD key and click Next.

In the next dialog box, you must choose the administration method. Choose Centralized Administration Through Network to allow the computer to access the Management Server for centralized management. Stand-Alone Installation will not allow the workstation to access the Management Server.

This option is useful for stand-alone gateways and servers that do not need to access the Management Server. In stand-alone installations, the configuration files must be copied manually to the host. See Chapter 4, “User Interface” on page 77. Click Next to continue.

In the next dialog box, you must choose the products to install.

---

8 F-Secure, 1999, F-Secure VPN+ 4.1, Gummerus Printing.
F-Secure Management Agent is the component used by all F-Secure products for transferring data to F-Secure Administrator via the Management Server and for fetching policies and certificates. After choosing the products to install, click **Next**.

In the next dialog box, you can change the folder where the software will be installed.

We recommend installing the software to the default destination folder **C:\Program Files\F-Secure**. Several subdirectories will be created, including a directory for program files and a directory for configuration files. Click **Next** to continue.

In the next dialog box, you will need to enter the path to the management key (**admin.pub**).

Click the **Browse** button to browse for the management key that was created during the F-Secure Management Tools setup. Click **Next** to continue.

Choose the communication method. This option depends on the installation you chose during the Management Tools installation. For small installations, the Communication directory can be used. For larger WAN connections, F-Secure Management Server is recommended.

Enter the path to the communication directory.
If you selected Communication Directory, you will need to enter a specific domain username and password. Enter this information, and click **Next** to continue.

Enter the HTTP address of the F-Secure Management Server. For example http://192.168.120.21. Note that you must use http:// in the beginning of the address.
Click **Next** to continue.

In the next dialog box, you are given the option to use a configuration disk. If you click **No**, F-Secure VPN+ will generate a private key for the host and submit a certification request to the Management Server. The host certificate is retrieved from the Management Server. Click **Next** to continue.

In the next dialog box, type in the host’s organization information. The host information will be used in the certification request. In the Country field, enter the two-digit country code (ISO standard 3166). In the Organization field, use only ASCII characters.
Click **Next** to continue.

In the Identity field, type in the IPSec identity of the host. This can be an IP address, a fully qualified domain name, or an e-mail address in the format User@F-QDN (Fully Qualified Domain Name).

The installation program automatically suggests E-mail Address as the identity if the host does not use static IP addresses (that is, if it is a dial-up host or uses DHCP to get the IP address).
If you use an e-mail address as the identity, you cannot be the responder in any kind of communication. For example, two clients using e-mail addresses for identification cannot communicate directly with each other using IPSec.

Do not use existing e-mail addresses. We recommend creating an e-mail address, for example “Computer18@vpn.company.com”.

A computer using User@FQDN as its identity must use Aggressive mode in an IKE negotiation, because the responder must decide whether to continue the negotiation based on the information contained in the first IKE packet. See the section “Aggressive Mode” on page 143.

In Main mode, the first packet contains only the IP address. In Aggressive mode, the identity is also included in the first packet. These IKE settings can be chosen when defining connections for the VPN. See the section “Creating Connection Templates” on page 47.

A list of changes that will be made to your system is displayed. Click Next to complete the setup.

The default installation folder is C:\Program Files\F-Secure.

The following subdirectories will be created:
\COMMON\ — Contains all of the F-Secure Management Agent executable files, admin.pub (the management public key), and policy.bpf (the base policy file). (The policy.bpf file will be copied later from the Management Server.)
\VPNPLUS\Program — Contains all of the executable files.
\VPNPLUS\Config — Contains the private key of the host, and the host certificate.

A readme.txt file will be placed in the root. After all the files are copied to the hard drive, you will be prompted to read the latest release information.

Next, you will be asked if you want to restart your computer. When you restart your computer, F-Secure VPN+ will be ready to run.

As can be seen on the instructions for the IPSec they are much more complicated than the instructions for the PPTP. The instructions are almost more confusing to the installation process of the protocol on the client, than of aid. The web page offers some aid to the most common questions and an e-mail address.

When the IPSec did not work, as it should according to the manual, a failure search was initiated.

1. To prevent that any mistakes had been made when the IPSec was installed and configured all inputs were double checked
2. The distribution was uninstalled and then reinstalled exactly following the instructions that were provided with the program.
3. A search through the manuals and on the F-Secure web page revealed nothing that could explain what was wrong.

As no IPSec connection could be established the manuals were searched for explanation of what could be wrong. The troubleshooting chapter had no explanation
of what could be wrong, even though it had various troubleshooting tips. The F-Secure manual was better formed than the PPTP manual in the aspect that it contained a troubleshooting part. The troubleshooting chapter did not come to any aid, as the problem that occurred did not have any explanations to it in the troubleshooting chapter. Although the chapter on troubleshooting contained various problems and their solutions, it did not contain the solution to the installation problem. That chapter contained the following sub chapters, none of which contained a solution to the problem:

Problem: Internal authentication failed.
Problem: Cannot connect to the other hosts using IPSec.
Problem: Cannot browse the network with Network Neighborhood or My Computer.
Problem: Cannot connect to a node in another network.
Problem: The VPN+ Gateway or Enterprise Gateway cannot be enabled to use a Management Server.
Problem: All connections between the nodes suddenly stop.
Problem: The nodes cannot connect to the Management Server.
Problem: I cannot connect to a server using NetBEUI or IPX/SPX.
Problem: Cannot connect to the other hosts using IPSec, and the following error message displays:

It was not possible to get the trials done even if the manual was followed exactly. The failure of completing the trials is mainly due to the following factors:

1. Late delivery of the program from Atremo AB, the F-Secure distribution partner in Sweden.
2. Insufficient time to implement the solution in the test lab, partly due to late delivery of the program and partly due to time restrictions on access to the test lab.
3. Equipment that was not fully compatible with some of the requirements that the program placed on both clients and server, i.e. memory requirements that resulting in occasional memory error message that sometimes caused the need to restart the computer.
4. The Internet Information Service (IIS) 4.0 needed to run the VPN solution from F-Secure was not included on the CD that came from F-Secure and had to be acquired elsewhere.

5.2 Transmission speeds
The aim of measuring transmission speeds was to see if there was any difference in transmission speeds depending on the file types and on the frame sizes. Obviously due to the fact that it was impossible to set up the lab environment it is impossible to acquire any measurement data from the experiment. Because there is no data it is impossible to compare the two protocols with respect to speed, bandwidth use and frame rate transfer with different frame sizes. However there is a study made by Juha Viinikainen at Sonera OY9 on the effectiveness of IPSec with a gateway-to-gateway connection on a 100 Mbps network. This study is not quite the same as the one that was planned for this work but it nevertheless gives an idea of the transmission speeds

---

between two computers with variable frame size. As previously pointed out the work here was focused around client/server environment and not gateway-to-gateway connection as Viinikainen has tested. The results however represent speeds that can be reached between two hosts on a 100 Mbps connection.

The Finnish study shows that depending on the frame size of the packets the transmission varies in speed. At the top of the table is the triple-DES algorithm that provides the strongest encryption available today for IPSec. It also indicates that the transmission speed is slowest at the strongest encryption speed. The triple-DES or 3DES encryption algorithm provides a 160-bit strong encryption. The Plaintext provides no encryption to the data that is transported. The strongest encryption is displayed at the top, with degrading encryptions until finally plaintext is sent. This is illustrated in Table 4.

<table>
<thead>
<tr>
<th>Frame size</th>
<th>64</th>
<th>128</th>
<th>256</th>
<th>512</th>
<th>1024</th>
<th>1280</th>
<th>1518</th>
<th>Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN + 3DES</td>
<td>2.5</td>
<td>2.7</td>
<td>6.0</td>
<td>6.2</td>
<td>9.7</td>
<td><strong>10.4</strong></td>
<td>9.3</td>
<td>Mbps</td>
</tr>
<tr>
<td>VPN + DES</td>
<td>2.9</td>
<td>4.6</td>
<td>8.5</td>
<td>12.9</td>
<td>16.5</td>
<td><strong>17.8</strong></td>
<td>17.0</td>
<td>Mbps</td>
</tr>
<tr>
<td>VPN + Blowfish</td>
<td>2.9</td>
<td>4.9</td>
<td>9.5</td>
<td>15.5</td>
<td><strong>22.6</strong></td>
<td>20.7</td>
<td>24.1</td>
<td>Mbps</td>
</tr>
<tr>
<td>VPN + bypass</td>
<td>4.6</td>
<td>9.2</td>
<td>17.9</td>
<td>34.3</td>
<td>41.2</td>
<td>43.5</td>
<td><strong>47.3</strong></td>
<td>Mbps</td>
</tr>
<tr>
<td>Plaintext NT</td>
<td>35.3</td>
<td>26.5</td>
<td>92.2</td>
<td><strong>95.5</strong></td>
<td>54.4</td>
<td>41.5</td>
<td>44.7</td>
<td>Mbps</td>
</tr>
</tbody>
</table>

Table 4. Test results from IPSec gateway-to-gateway testing.

The results clearly show that transmission speeds vary greatly depending on what encryption is used and sizes of frames. The strongest encryption algorithm is placed at the top in the table and then they gradually weaken until a plaintext is sent showing maximum speed at frame size 512. While the strongest algorithm, i.e. 3DES shows fastest transfer rate at frame size 1280. So depending on the encryption algorithm a frame size should be decided. The data from the table is presented in a graphical form in figure 13.
**VPN with encryption algorithms**

![Graphical presentation of table 4.](image)

**Figure 13.** Graphical presentation of table 4.

The test environment was built with four computers, a plaintext computer connected to a VPN gateway, which in turn was connected to another gateway and that gateway was connected to another plaintext computer. This is illustrated in Figure 14. Secure Hash Algorithm (SHA) and pre-shared keys were used in all tests conducted by Vii nikainen. According to Vinnikainen all test were made twice, once for both directions. Better result of the two tests was selected as a final result. Result means maximum transmission speed where no packet was lost. The gateway equipment was Intel PC 333 MHz Pentium II, 128 Mb memory, NT 4.0 with SP3, and 3Com network cards.

![Connection of 2 plaintext computers through VPN gateways.](image)

**Figure 14.** Connection of 2 plaintext computers through VPN gateways.

The F-Secure company states that the performance of their VPN+ program depends on the MHz of the processor that the computer has\(^\text{10}\). The encryption performance is quite linear according to Vinnikainen, so with a PIII-500MHz they would expect 35-40 Mbps performance with the Blowfish encryption algorithm (128bit) as compared to about 20-22 Mbps with the 333 MHz Pentium II. Which is a 50% increase in MHz of the processor that results in a 75% - 81% increase in encryption speed.

5.3 Security of the two protocols
The aim of this chapter is to analyse the security aspects of the two protocols, their strengths and weaknesses, and where they are most vulnerable against attacks. The two protocols vary on security and levels in the OSI model. They are working on two different levels in the OSI model and that gives two different types of vulnerability and protection of the two protocols.

5.3.1 The PPTP security aspects
One of the biggest benefits of the PPTP protocol is the possibility to transport other protocols than just TCP/IP protocol, such as IPX and NetBEUI by encapsulating them into a new TCP/IP packet before sending the packet away. Perhaps the biggest drawback of the PPTP protocol is that it must connect to a NT server since the PPTP protocol was invented and produced by Microsoft and can only be run on the computer platforms that were created by Microsoft, i.e. Windows 95/98 and Windows NT. No literature states anything about the new Windows 2000 operative system.

According to an article from Network Week by Steve Ranger\textsuperscript{11} on the F-Secure homepage there are several serious flaws in the NT tunnelling protocol. Microsoft denies that such a problem exists with the PPTP protocol. David Bridger, the British product manager for NT says, “this appears to be quite speculative, we can not see where the security risk is”. But Neil Cooper, IT security services senior manager says that it is easy for a person with access to the net and a sniffer program should be able to pick up the handshake between the client and the server and use that as a starting point to break the encryption.

The control channel messages are neither authenticated nor protected, allowing for attacker to take control of the underlying TCP connection. Once that is accomplished there are no problems to forge control channel messages and alter the genuine messages without being detected. The Generic Routing Encapsulation (GRE) packets are also not protected with any cryptography. So with the right tools and with the right knowledge it is not difficult to attack and manipulate a communication link that has been established with PPTP (Brown, 1999).

Attacks against cryptographic algorithms such as DES and Blowfish can be divided into 3 main categories

- Attacks against the algorithms
- Attacks against the protocol
- Attacks against the implementation

The algorithm could make the whole system weak. Using weak keys, using small of data sizes and altering hash functions contribute to a weaker algorithm. The encryption algorithms and key exchange protocols does not guarantee safety by themselves. Choosing an insecure seed for the key to be based on destroys the protocol. With a combination of keys the security is also jeopardised, as a strong key combined with a weak key jeopardises the stronger key, thus the whole system gets

\textsuperscript{11} Ranger, S., 1998, NT Tunnelling product is insecure, expert says, [online], Available: http://www.fsecure.com/support/misc/vpn_vs_pptp.html [Accessed May 16\textsuperscript{th} 2000]
compromised. The main attacks against the implementation are though through key recovery, sometimes called back doors into systems in case someone forgot the password.

Point to Point Protocol (PPP) packets are encapsulated inside a GRE packet; the GRE packets do not have sequence numbering making them vulnerable to spoofing attacks by desynchronising GRE channel. Another attack is against the passwords as they are sent to the server after they have been hashed. Since the passwords are changed to uppercase letters for the first hashing they are vulnerable to dictionary attacks which in turn compromises the second hashing function. A challenge handshake from the server, where the server challenges the request from the client, results in a new answer from the client. The answer is then compared to a database on the server and if the hashing values match the server will accept the connection. Although this eliminates the dictionary attack it is still vulnerable for hashing functions attacks.

Yet another vulnerability of the PPTP algorithm is that it relies on Point-to-Point Protocol (PPP). PPP is responsible for setting up and initialising the communication parameters that are to be used during the communication session. Since PPP does not authenticate the packets it is possible to do a man-in-the-middle attack, where the attacker listens to all messages going back and forth between the hosts and can take over the communication or forge it. Another attack is the spoofing attack, where the attacker assumes the identity of a third party; these attacks can easily be avoided by configuring the router not to pass unauthorized traffic. Since Windows 95 only has minimal security measurements it is extremely vulnerable for attacks and should be traded for higher security operative system such as Windows NT.

There already is a program that is specifically designed to sniff up PPTP traffic and to analyse it. This program is available at L0hpt homepage and it is called “L0hpt sniffer”, and it is designed to analyse authentication packets and to generate challenge-hashing value on the password to send back to the server. Until recently only 40-bit encryption was allowed outside of the U.S., which is very weak.

5.3.2 The IPSec security aspects
The IPSec protocol is not produced by only one manufacturer but is decided upon by the Internet Engineering Task Force (IETF) making it possible for multiple vendors to compete on the IPSec market. Which can cause interoperability problems between different programs that use the IPSec protocol. The IPSec protocol also supports multiple types of encryption algorithms and accommodates developing algorithms.

There are several problems that plague the IPSec protocol in terms of security. Static keys used in IPSec and the difficulty in exchanging static keys leads to scalability difficulties, as it is difficult to manage thousands of symmetric keys in large networks. The encapsulation approach can also cause problems as it increases the size of the IP packet and can cause a spill over to a new packet (Brown, 1999).

IPSec can be attacked and compromised just like PPTP. The largest category of attacks is the category of attacks against implementation as the vendors have accepted a weaker key, the so-called “NULL” key or no key, in one direction at a time. This compromises the stronger key that is needed during the communications between the computers (Brown, 1999).
Analysis

Key management attacks are possible as there is no true interoperability between the vendors. Under the Internet Key Exchange protocol (IKE) specification, any side could terminate the connection and another computer could take over as the receiver, spoofing the identity of the original host, of the data from the transmitting computer. This attack is similar to TCP session hijacking (Brown, 1999).

IPSec has no methods to authenticate the user, no access rights, and no verification etc. so anyone with access to a host can access another host by pretending to be the rightful user of the host. IPSec does not mandate the use of authentication or encryption thereby increasing the possible weaknesses of the IPSec protocol to provide a protection for the data (Brown, 1999).

The IPSec protocol and the PPTP protocol are on different layers of the OSI model. The IPSec protocol is on the network layer while the PPTP is on the data link layer. This means that they can actually be applied together to provide even stronger encryption than was possible while they were apart (Brown, 1999).

The biggest weaknesses of the IPSec protocols according to Kosiur (1998) are the lack of user management; lack of vendor interoperability so if two companies apply IPSec solutions from different vendors there is no guarantee for it that they will work together; finally little desktop support in case of troubles which was noticeable during the trials when the program did not function properly.

5.3.3 Security comparison

To compare the security aspects of the protocols without setting them up in a table is almost impossible. Therefore a short summary of the protocols and the strengths and drawbacks of each protocol will be presented in a table. The table is not exhaustive but merely to give an idea of the differences of security strengths and weaknesses of the two protocols.
<table>
<thead>
<tr>
<th></th>
<th><strong>PPTP</strong></th>
<th><strong>IPSec</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
<td>- Multi protocol transport</td>
<td>- Accommodates developing encryption algorithms</td>
</tr>
<tr>
<td></td>
<td>- User authentication</td>
<td>- Sequence numbering</td>
</tr>
<tr>
<td><strong>Weaknesses</strong></td>
<td>- Demands NT server termination</td>
<td>- Desktop support</td>
</tr>
<tr>
<td></td>
<td>- Weak handshake</td>
<td>- Product interoperability</td>
</tr>
<tr>
<td></td>
<td>- Control message not encrypted</td>
<td>- User management</td>
</tr>
<tr>
<td></td>
<td>- Possibility to use weak keys</td>
<td>- Possibility to use weak keys</td>
</tr>
<tr>
<td></td>
<td>- No sequence numbering on GRE packets</td>
<td>- No user authentication</td>
</tr>
<tr>
<td></td>
<td>- Low quality encryption outside of USA.</td>
<td>- Static keys and key exchange</td>
</tr>
<tr>
<td></td>
<td>- Relies on PPP</td>
<td></td>
</tr>
<tr>
<td><strong>Most common</strong></td>
<td>- Hashing attacks</td>
<td>- Strong/weak key combination</td>
</tr>
<tr>
<td>attacks against</td>
<td>- Handshake attacks</td>
<td>- Key management attacks</td>
</tr>
<tr>
<td>the protocol</td>
<td>- Strong/weak key combination</td>
<td>- Brute force</td>
</tr>
<tr>
<td></td>
<td>- Spoofing</td>
<td>- Dictionary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Spoofing</td>
</tr>
</tbody>
</table>

**Table 5.** A summary of the security aspects of PPTP and IPSec.
6 Conclusion

The aim of this project was to compare and contrast two of the protocols that dominate the VPN market today, i.e., the Point-to-Point Tunnelling Protocol (PPTP) produced and distributed by the Microsoft Corporation, and the IPSec protocol, which is produced by many vendors.

The emphasis of this work was placed on comparing the protocols with respect to:

1. Ease of installing the applications on the hosts and to establish contact.
2. Encryption speed, traffic flow and bandwidth usage. For example to inspect if it made any difference if the packets were of different sizes when the packets were encrypted.
3. The security aspects of the two solutions.

As previously pointed out in chapter 3, the Microsoft PPTP protocol should be very easy to install and administer. It is easier said than done to implement PPTP in a system that is supposed to work. PPTP requires skills and more than any other thing time. Time to implement the solutions representing the real world that was created and to successfully establish a PPTP connection between the clients and server. Time to solve the problems that surface during the installation and time to fix those problems. The PPTP lab never got fully functional. This resulted in that no test was actually done on the PPTP network because it did not work. The most likely reason for the PPTP lab failure is some kind of hashing problems with 128-bit encryption and the RAS service of the operating systems, which resulted in that no trials were made with the PPTP.

“Security problems on the Internet [...] F-Secure VPN is an easy, cost-effective, fast and complete solution to this problem” Jussi Partanen, Marketing Manager, Nexor System Service.12

The F-Secure VPN+ program from F-Secure proved to be more complicated to install and run than the manual indicated. There were problems already during the installation of the F-Secure suite. With missing components that were required for the installation and inadequate manual as explained in chapter 5, it proved to be impossible to complete the setup of the IPSec protocol and to test it. The timeframe did not allow for any more research of the problem and to acquire all the missing components as no extra memory modules could be obtained in time. The Internet Information Services 4.0 could be found on the Microsoft web pages and were downloaded from there. This resulted in that no measurements of the transmission speeds could be performed. These results meant that no comparison of these two protocols could be made, as there was no data available to compare them against each other.

Perhaps the most interesting part of the exam work is the comparison made by Viinikainen where he compares several different encryption algorithms in an IPSec

environment. There he clearly states that to the user, the VPN should appear to be transparent up to a 10 Mbps LAN network with triple DES encryption algorithm. This implies that IPSec could be used on the network to protect the data on the LAN as well as on the Internet.

It is important to remember that VPN should only be a part of the security measures that should be taken to prevent unauthorized access and that security is only as strong as the weakest part of the chain. There are security compromises in VPN networks today that can give a false sense of security if the protocols are not correctly implemented for maximum security.

The final conclusion of this work is that is more complicated to install and use a VPN solution than what the manufacturers claim. The manufacturers supply inadequate information and installation guidelines for the work to be done without technical assistance from the manufacturers or vendors, as explained previously in this report.

6.1 Suggestions for future work

An interesting aspect to look at would be the scalability of the two solutions. That is to see if both solutions scale well with increased number of users. The scale of such test makes it almost impossible to acquire the equipment, the space and the time needed to complete such a test in four months. Another way to test these systems is to test them under extreme pressure with multiple clients performing heavy file exchanges with the server during encryption session. The performance of the participating clients and servers could then be measured to see if it flattens out at any given point. This again requires large amount of equipment that is difficult to acquire and a large amount of time dedicated to testing the equipment. Both of these requirement lie outside of what is possible within the timeframe of this work and are therefore suggested as a future work.

There are several ways to test a VPN network one is to test the scalability, i.e. how well a VPN system scales up to many users. This is difficult if not impossible in a small test laboratory, and may require hundreds of hours to set up, implement and measure. There is therefore no possibility to test the scalability of VPN solutions in this work. Another way to test VPN solutions is to test how many clients can utilize a server and either download or upload extensive amount of information to the server at the same time. The performance of the server could then be measured to see how well the server handles multiple clients with encrypted connections at the same time.

It would of course be very interesting to get a fully functional lab to work as described in the work and to perform the planned tests in the test lab as described. To perform similar test with the L2TP protocol against the other two protocols that have been tested in this paper. With emphasis on testing encryption speed and security and to compare the installation of the L2TP protocol to the troublesome installation of the PPTP and IPSec protocols. An explanation of the netXray measurement tool that could be used to measure the traffic follows in chapter 6.1.1 along with an explanation of how to measure the traffic on the net. A suggestion of a testing simulation is explained in chapter 6.1.2 where a suggestion of file types and frame sizes are made for testing the protocols.
6.1.1 NetXray

NetXray is a program that is produced by Network Associates International (NAI). NetXray is used to measure traffic on a LAN, it can be specified to handle only selected computers or to listen to all the traffic on the net. It is possible to listen to certain protocols such as FTP (File Transfer Protocol) or SNMP (Simple Network Management Protocol) or sniff up any level of the OSI model introduced earlier. The program has many options and possibilities. A few examples include\textsuperscript{13}:

- Monitoring of network statistics
  - Utilization \%
  - Bytes
  - Frame size distribution
- Error statistics
  - Number of errors
  - Oversized frames
- Protocol statistics
  - Network utilization \% by protocol
- Frame size statistics
  - \% Of frames by frame size

The only portion of the program that was be used in this work was the listening and measurement function of the netXray program. A measurement of the number of packets sent or received and how long time the transfer took. The time and packet information’s are possible to extract with the netXray program. This was not done due to installation difficulties of the protocols.

The netXray program should be installed on a computer that is connected to a hub and is set to measure several different factors during the transmission, those being:

1. Traffic going to and from specific IP addresses. The program will count the number of packets going between the two IP addresses.
2. Measure the time that the transmission takes and the transmission speed between the two IP addresses.
3. Measure frame rate and utilization of the network and the computer.
4. Give detailed information in statistical tables and graphical images over the traffic during the measurement period.

The connection of the measuring computer is illustrated in Figure 13.

\textsuperscript{13} A full description of the program capabilities is available at http://www.nai.com
Figure 15. The test lab setup with the measuring computer.

6.1.2 Simulation settings

The simulation should put two different programs, PPTP from Microsoft and VPN+ from F-Secure. First a trial of the PPTP solution will be tried and then the VPN+ solution.

The sniffer program should listen to the traffic between the two communicating computers and then present the results in a graph showing how much traffic passed through during specific time interval. The netXray analyses the type of traffic, i.e. TCP/IP or IPX that was used. It also measures the duration of the traffic and how much data was passed between the two computers.

The simulation is set up on two different nets, one called the local net which gets an IP numbers in class A range (10.10 etc.). Class A range address is where 8 bits of the 32 bit address integer are used as network identifier and the remaining 24 bits as the host identifier. The external network gets IP addresses in the C class range (193.10 etc.). Class C range address is where 24 bits are used as a network identifier and the remaining 8 bits as host identifier (Halsall, 1996). The local net is only composed of a single client computer connected to the server through a 10 Mbps hub. The external net is connected to the college network at 10 Mbps through switches and routers to the modem-pool server.

The trials are set up to measure the following file type transfers:

1. Video feed
2. Digital medical image
3. Sound file
4. Text file
5. Different frame sizes

These file formats were chosen as they represent the many different types of files that are sent through a network every day. All from a video feed that can be live or replay to simple sound files or text files, which may be the most common files that are transferred today.
To achieve this transfer it is necessary to setup the test lab and to see that the following items are functioning properly. Then the trials of the PPTP and IPSec can be initiated:

1. The PPTP trial
   a) The connection of the server to the client on the LAN via the hub has to function properly before the trials of the protocols begin, i.e. it must be possible to ping both the server and the client.
   b) The connection of the server to the client that is connected by modem has to function properly before the trials of the protocols begin, i.e. it must be possible to ping both the server and the client.
   c) A trial of the PPTP protocol both for LAN and modem connection, with the previously listed file types.
   d) The data that is collected by the sniffer program and the information about the test lab is then gathered and put together as a result of the PPTP trial.

2. The IPSec trial
   b) The connection of the server to the client on the LAN via the hub has to function properly before the trials of the protocols begin, i.e. both client and server must respond to ping messages.
   c) The connection of the server to the client that is connected by modem has to function properly before the trials of the protocols begin, i.e. both client and server must respond to ping messages.
   d) A trial of the IPSec protocol both for LAN and modem connection, with the file types listed previously.
   e) The data that is collected by the sniffer program and the information about the test lab is then gathered and put together as a result of the IPSec trial.

3. Collection of the data that is gathered with the sniffer program during the trials and presentation of the information on the trials.
Acknowledgement

My thanks to Bengt Berg, head of roentgen department, Skaraborgs Regional Hospital, KSS and his staff for lending out digital roentgen pictures. To Mikael Berndtsson for his patience and support as a supervisor. To Anders Petterson, Johan Petterson and Björn Erlendsson at the University IT-department for their help and assistance. To the department of health at the University of Skövde, for lending the computers needed.
References


Andersson, N., 1999, February 9th, Ta tunnelbanan genom Internet, Nätverk och kommunikation, Pages 52-54, IDG, Stockholm.


Kosirur, D., 1998, Building and managing VPNs, John Wiley & Sons, Massachusetts, USA.

Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Explanation</th>
<th>First page occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>AH</td>
<td>Authentication Header</td>
<td>(4)</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
<td>(9)</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
<td>(17)</td>
</tr>
<tr>
<td>DES-CBC</td>
<td>DES with Cipher Block Chaining</td>
<td>(6)</td>
</tr>
<tr>
<td>DUN</td>
<td>Dial Up Networking</td>
<td>(28)</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulated Security Protocol</td>
<td>(4)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation Protocol</td>
<td>(9)</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
<td>(35)</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services</td>
<td>(31)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange protocol</td>
<td>(35)</td>
</tr>
<tr>
<td>IPSec</td>
<td>IP Security Protocol</td>
<td>(2)</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
<td>(10)</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
<td>(10)</td>
</tr>
<tr>
<td>L2F</td>
<td>Layer 2 Forwarding</td>
<td>(9)</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
<td>(3)</td>
</tr>
<tr>
<td>MPPE</td>
<td>Microsoft Point-to-Point Encryption</td>
<td>(10)</td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interface</td>
<td>(3)</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
<td>(9)</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
<td>(1)</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
<td>(9)</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
<td>(2)</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
<td>(10)</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Service</td>
<td>(11)</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure Multipurpose Internet Mail Extensions</td>
<td>(1)</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
<td>(4)</td>
</tr>
<tr>
<td>SPI</td>
<td>Security Parameter Index</td>
<td>(4)</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
<td>(1)</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
<td>(4)</td>
</tr>
</tbody>
</table>